Best Available Copy

W157 (3)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-204701

(43)Date of publication of application : 09.08.1996

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/54
H04L 12/58
H04L 12/22
// G09C 1/00

(21)Application number : 07-010741

(22)Date of filing : 26.01.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

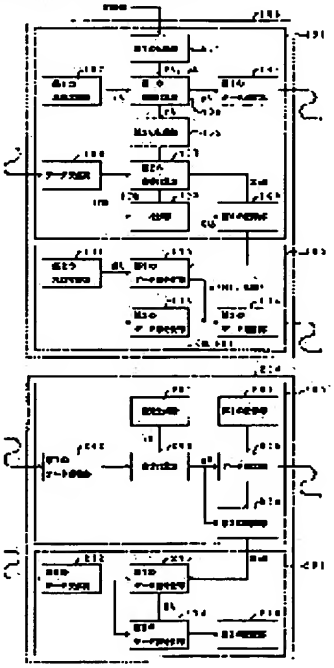
(72)Inventor : UEDA HIROKI
MIYAGUCHI SHOJI

(54) ELECTRONIC MAIL CIPHER COMMUNICATION SYSTEM AND CIPHER COMMUNICATION METHOD

(57)Abstract:

PURPOSE: To enhance the security of transmission data for transmission and reception terminal equipments by holding a key in common for the transmission terminal equipment and the reception terminal equipment and to cipher the data and to send/receive the data so as to disable leakage of information through intentional monitoring of communication data by a 3rd party.

CONSTITUTION: A random number generator 102 of a terminal equipment A generates a random number rA in 512 bit length and gives the random number to a power multiplier 103. The random number rA is stored in a storage section 105 for a 2nd use. The power multiplier 103 extracts a prime PA and a primitive root gA from the storage section 101 and uses the random number rA received from the random number generator 102 to calculate power multiplication and generates a public-key yA of the terminal equipment A and transfers it together with the prime PA and the primitive root gA to a transmission section 10, which sends them to a terminal equipment B. The terminal equipment B uses a random number rB and uses a computer 203 to conduct the power multiplication calculation to obtain a prime PB and a primitive root gB. Furthermore, the terminal equipment B sets an identifier IDB and a public-key of the terminal equipments A, B and stores them in a storage section 206. The terminal equipment B sends the key yB and the identifier ID to the terminal equipment A via a transmission section 205. A comparator 108 of the terminal equipment A compares the IDA with the IDB to confirm whether or not the relation of KA=KB is in existence.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－204701

(43)公開日　平成８年(1996)８月９日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00				
9/10				
9/12				
			Ｈ０４Ｌ　9/ 00　Ｚ	
		9466－5K	11/ 20　１０１　Ｂ	

審査請求　未請求　請求項の数10　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願平7－10741

(22)出願日　平成７年(1995)１月26日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　植田　広樹
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　宮口　庄司
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

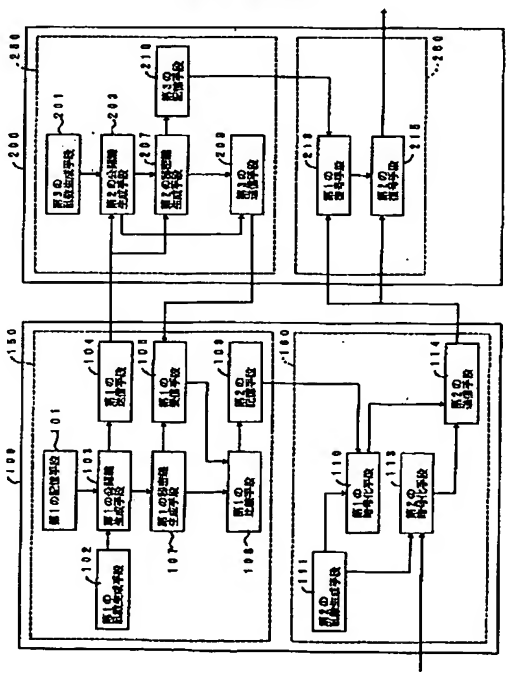
(54)【発明の名称】　電子メール暗号通信システム及び暗号通信方法

(57)【要約】

【目的】　本発明の目的は、第３者による意図的な通信データ監視による情報漏洩を不可能にし、送信側端末と受信側端末間における送信データの機密性を高めることが可能な電子メール暗号システム及び暗号化装置を提供することである。

【構成】　本発明は、受信端末200 が共通鍵を生成するためのデータを送信し、受信したデータに基づいて共通鍵を生成し、共通鍵の部分鍵を送信端末100 に送信する共通鍵生成処理手段150,250 と、共通鍵生成処理手段150 により生成された共通鍵を用いて暗号文を生成し、受信端末に送信し、受信端末が暗号文を共通鍵を用いて復号化するデータ転送処理手段160,260 とを有する。

本発明の原理構成図



【特許請求の範囲】

【請求項１】　暗号化された文書を送信する送信端末と、該送信端末より受信した文書を復号化する受信端末より構成される暗号通信システムにおいて、

前記受信端末と前記送信端末との間で共有する共通鍵を生成するためのデータを前記送信端末に送信し、受信したデータに基づいて共通鍵を生成し、生成された該共通鍵の部分鍵を前記送信端末に送信し、前記送信端末側で該部分鍵に基づいて共通鍵を生成する共通鍵生成処理手段と、

前記共通鍵生成処理手段により生成された前記共通鍵を用いて、暗号文を生成し、前記受信端末に送信し、前記受信端末が該暗号文を前記共通鍵を用いて復号化するデータ転送処理手段とを有することを特徴とする電子メール暗号通信システム。

【請求項２】　前記共通鍵生成処理手段において、

前記送信端末は、

予め装置毎に定めたｎビットの素数P_A、該素数P_Aの原始根g_Aを保持する第１の記憶手段と、

乱数r_Aを生成する第１の乱数生成手段と、

前記第１の記憶手段より前記素数P_A、原始根g_Aを取り出し、さらに、前記乱数r_Aを用いて巾乗演算を行い、第１の公開鍵y_Aを生成する第１の公開鍵生成手段と、

前記素数P_A、前記原始根g_Aを前記第１の公開鍵生成手段より生成された前記第１の公開鍵y_Aと共に他装置に送信する第１の送信手段と、

前記他装置から、前記他装置で生成された共通鍵の一部である部分鍵ID_B及び第２の公開鍵y_Bを受信する第１の受信手段と、

前記第１の受信手段により受信した前記第２の公開鍵y_Bと前記第１の公開鍵生成手段で用いた前記素数P_A、前記原始根g_Aにより巾乗演算を行い、第１の鍵K_Aを生成する第１の秘密鍵生成手段と、

前記第１の鍵K_Aの一部分を部分鍵ID_Aとし、該部分鍵ID_Aと前記部分鍵ID_Bを比較する第１の比較手段と、

前記第１の比較手段による比較の結果、一致する場合には、前記第１の鍵K_Aのビット列のうち、前記部分鍵ID_Aにした部分とは異なる一部分を共通鍵K_{AB}として、該共通鍵K_{AB}を記憶する第２の記憶手段とを有し、

前記受信端末は、

乱数r_Bを生成する第３の乱数生成手段と、

前記送信端末から送信された前記素数P_A，前記原始根g_A及び公開鍵y_A、及び前記乱数r_Bを用いて巾乗演算を行い、前記第２の公開鍵y_Bを生成する第２の公開鍵生成手段と、

前記第２の公開鍵生成手段で生成された前記第２の公開鍵y_B、前記素数P_A、前記乱数r_Bにより巾乗演算を行い、第２の鍵K_Bを生成する第２の秘密鍵生成手段と、

前記第２の秘密鍵生成手段により生成された第２の鍵K_Bのビット列の一部分を部分鍵ID_Bとし、第２の鍵K_Bのビット列のうち、該部分鍵ID_Bに使用した部分以外の一部分を共通鍵K_{AB}として格納する第３の記憶手段と、

前記第２の公開鍵y_B及び前記部分鍵ID_Bを前記送信端末に送信する第３の送信手段とを有する請求項１記載の電子メール暗号通信システム。

【請求項３】　前記送信端末は、

乱数R_Aを生成する第２の乱数生成手段と、

前記乱数R_Aで前記第２の記憶手段に格納されている前記K_{AB}を暗号化し、第１の暗号文Ｅ（K_{AB}，R_A）を生成する第１の暗号化手段と、

前記乱数R_Aで本文Ｍを暗号化し、第２の暗号文Ｅ（Ｍ，R_A）を生成する第２の暗号化手段と、

前記第１及び第２の暗号化手段で生成された前記第１の暗号文Ｅ（R_A，K_{AB}）及び前記第２の暗号文Ｅ（Ｍ，R_A）を送信する第２の送信手段とを有し、

前記受信端末は、

前記送信端末から受信した前記第１の暗号文Ｅ（K_{AB}，R_A）を用いて、前記第３の記憶手段に格納されている前記共通鍵K_{AB}を用いて復号し、復号鍵R_Aを取得する第１の復号手段と、

前記復号鍵R_Aを用いて、前記第２の暗号文Ｅ（Ｍ，R_A）を復号化して本文Ｍを取得する第２の復号手段とを有する請求項１記載の暗号通信システム。

【請求項４】　前記送信端末は、

前記本文Ｍのビット長を所定のビット列に変換し、変換データＭＩＣを送信する変換・送信手段を有し、

前記受信端末は、

前記変換データＭＩＣを受信すると、前記第２の復号化手段により取得した本文Ｍのビット長を所定のビット列に変換し、変換データＭＩＣ’を生成する第１の変換手段と、

前記第１の変換手段により取得した変換データＭＩＣ’と受信した前記変換データＭＩＣとを比較し、一致するかを判断する第２の比較手段とを更に有する請求項３記載の電子メール暗号化システム。

【請求項５】　前記送信端末は、

前記本文Ｍのビット長を所定のビット列に変換し、変換データＭＩＣを生成する第２の変換手段と、

前記変換データＭＩＣと前記第２の乱数生成手段で生成された前記乱数R_Aを暗号化し、第３の暗号文Ｅ（ＭＩＣ，R_A）を生成する第３の暗号化手段と、

前記第３の暗号文Ｅ（ＭＩＣ，R_A）を送信する第４の送信手段とを有し、

前記受信端末において、

前記第４の送信手段により送信された前記第３の暗号文Ｅ（ＭＩＣ，R_A）を、前記第１の復号手段により取得

した前記復号鍵R_Aを用いて前記第３の暗号文Ｅ（ＭＩＣ，R_A）を復号し、データＭＩＣを取得する第３の復号手段と、
前記第３の復号手段により取得した前記ＭＩＣと、前記第２の復号手段により取得された前記本文Ｍとを比較して一致するかを判断する第３の比較手段を更に有する請求項３記載の暗号化システム。
【請求項６】　暗号化された文書を送信端末から電子メールで受信端末に送信し、該受信端末が該送信端末より受信した文書を復号化する暗号通信方法において、
最初に、共通鍵生成処理として、
前記送信端末が前記受信端末に対して、共通鍵を生成するためのデータを送信し、
前記受信端末が、前記データを用いて共通鍵を生成し、該共通鍵の部分鍵を前記送信端末に送信し、
前記送信端末は、受信した前記部分鍵と、前記送信端末で生成した鍵とを比較して一致していれば、前記部分鍵を前記送信端末及び前記受信端末間において共通に使用する正当な共通鍵として保持し、
次に、データ転送処理として、前記共通鍵生成手段において、正当な共通鍵であることが確認された後、
前記送信端末は、前記共通鍵を用いてデータを暗号化して、前記受信端末に送信し、
前記受信端末は、前記共通鍵を用いて暗号化されたデータを復号することを特徴とする暗号通信方法。
【請求項７】　前記共通鍵生成処理において、
前記送信端末は、予め、素数P_A、該素数P_Aの原始根g_Aを保持しておき、
前記送信端末は、乱数r_Aを生成し、前記素数P_A、前記原始根g_Aにより公開鍵y_Bを生成して前記受信端末に送信し、
前記受信端末は、乱数r_Bを生成し、前記送信端末より送信された前記素数P_A、前記原始根g_Aにより公開鍵y_Bと鍵K_Bを生成すると共に、該鍵K_Bのある特定部分のｍビットを共通鍵K_{AB}として保持し、該鍵K_Bの前記ｍビット以外のｎビットを部分鍵ID_Bとして、該公開鍵y_Bと共に前記送信端末に送信し、
前記送信端末は、前記受信端末より受信した前記公開鍵y_Bと予め保持されている前記素数P_A、前記原始根g_Aを用いて鍵K_Aを生成し、該鍵K_Aのある特定部分のｎビットを部分鍵ID_Aとし、該部分鍵ID_Aと前記鍵ID_Bが一致しているかを検査し、
一致している場合には、前記鍵K_Aと前記鍵K_Bが等しいと見做し、前記鍵K_Aのある特定部分のｍビットを共通鍵K_{AB}として保持する請求項６記載の暗号通信方法。
【請求項８】　前記データ転送処理において、
前記送信端末は、乱数R_Aを生成し、
前記乱数R_Aで前記共通鍵K_{AB}を暗号化し、暗号文Ｅ（R_A，K_{AB}）を生成し、
前記乱数R_Aで本文Ｍを暗号化し、暗号文Ｅ（Ｍ，R_A）を生成し、前記暗号文Ｅ（R_A，K_{AB}）と該暗号文Ｅ（Ｍ，R_A）を前記受信端末に送信し、前記受信端末に送信し、
前記受信端末は、前記共通鍵K_{AB}を用いて前記暗号文Ｅ（R_A，K_{AB}）を復号化して復号鍵R_Aを取得し、該復号鍵R_Aにより前記暗号文Ｅ（Ｍ，R_A）を復号し、本文Ｍを取得する請求項６記載の暗号通信方法。
【請求項９】　前記データ転送処理において、
前記送信端末は、
前記本文Ｍをある長さのｓビット列に変換し、変換されたデータをデータＭＩＣとし、該データＭＩＣを前記受信端末に送信し、
前記受信端末は、
前記データＭＩＣを受信し、前記復号化された前記本文Ｍをある長さのｓビット列に変換し、データＭＩＣ’とし、
受信した前記データＭＩＣと前記データＭＩＣ’を比較して一致するか否かを判定する請求項８記載の暗号通信方法。
【請求項１０】　前記データ転送処理において、
前記送信端末は、
前記本文Ｍをある長さのｓビット列に変換し、変換されたデータをデータＭＩＣとし、前記乱数R_A及び該データＭＩＣを暗号化し、暗号文Ｅ（ＭＩＣ，R_A）を前記受信端末に送信し、
前記受信端末は、
前記復号鍵R_Aを取得し、前記本文Ｍを取得した後に、前記本文Ｍをｓビット列に変換し、変換データＭＩＣ’を取得し、
受信した前記暗号文Ｅ（ＭＩＣ，R_A）を復号した復号文ＭＩＣを取得し、
前記変換データＭＩＣ’と前記復号文ＭＩＣを比較し、一致するか否かを判定する請求項８記載の暗号通信方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、電子メール暗号通信システム及び暗号通信方法に係り、特に、暗号化したデータを電子メールにより通信相手先に送信し、受信した電子メールを復号化する電子メールシステム上で、暗号通信を行う電子メール暗号通信システム及び暗号通信方法に関する。
【０００２】近年、ネットワークが全世界的に広がり、基本的なコマンドを使用して端末間でテキストデータを送受信するメールシステムが使用されている中で、送信データの内容の漏洩を防止することが可能な電子メール暗号通信システム及び暗号通信方法が望まれている。
【０００３】
【従来の技術】図１２は、従来の２端末間のデータ転送の例を示す。同図に示す例は、ある端末Ａからデータ

が電子メールにて送信され、受信する端末を端末Ｂとし、端末Ａ，Ｂ間が通信回線で直結している例である。この例の場合には、通信回線で、両端末が直結されているため、データＭの内容が漏洩することなしに、受信者である端末Ｂに送信される。

【０００４】図１３は、従来の端末群内におけるデータの例を示す。同図に示す例は、ある端末Ａから直接通信可能な端末群より１つの端末Ｃを選択し、データＭを電子メールにて送信する。次に、端末Ａからデータ Ｍを受信した端末Ｃは、端末Ｂと直接通信可能なら、データＭが最終的な送信先端末Ｂへ登録するためには、幾つかの端末を中継して送られる。なお、中継端末の選択は、電子メールシステムにおける経路制御と呼ばれるアルゴリズムによって制御される。

【０００５】

【発明が解決しようとする課題】しかしながら、上記従来のメールシステムを利用してデータを送受信する場合、以下のような問題がある。即ち、送信側端末と受信側端末との間に幾つかの中継端末が存在しており、送信されるデータは、その中継端末間をそのままの形態で通過するために、中継端末上で、第３者の意図的な操作によるデータ内容の漏洩が可能性として生じる。さらに、ネットワークを構成している中継回線を第３者が直接監視した場合でも、データ内容を知ることが可能である。このため、ネットワークが発達した現在において、メールシステムによる機密性の高い情報を含んだデータを受信するには危険が伴うという問題がある。

【０００６】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、中継端末上または、中継回線において、第３者による意図的な通信データ監視による情報漏洩を不可能にし、送信側端末と受信側端末間における送信データの機密性を高めることが可能な電子メール暗号通信システム及び暗号通信方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】図１は、本発明の原理構成図である。本発明は、暗号化された文書を送信する送信端末１００と、送信端末１００より受信した文書を復号化する受信端末２００より構成される暗号通信システムにおいて、受信端末２００と送信端末１００間において共通する共通鍵を生成するためのデータを受信端末２００に送信し、受信したデータに基づいて共通鍵を生成し、共通鍵の部分鍵を送信端末１００に送信し、送信端末側で部分鍵に基づいて共通鍵を生成する共通鍵生成処理手段１５０、２５０と、共通鍵生成処理手段１５０により生成された共通鍵を用いて、暗号文を生成し、受信端末に送信し、受信端末が暗号文を共通鍵を用いて復号化するデータ転送処理手段１６０、２６０とを有する。

【０００８】本発明において、共通鍵生成処理手段１５０は、送信端末１００が、予め装置毎に定めたｎビットの素数P_A、素数P_Aの原始根g_Aを保持する第１の記憶手段１０１と、乱数r_Aを生成する第１の乱数生成手段１０２と、第１の記憶手段１０１より素数P_A、原始根g_Aを取り出し、さらに、乱数r_Aを用いて巾乗演算を行い、第１の公開鍵y_Aを生成する第１の公開鍵生成手段１０３と、素数P_A、原始根g_Aを第１の公開鍵生成手段１０３より生成された第１の公開鍵y_Aと共に他装置に送信する第１の送信手段１０４と、他装置２００から、他装置の部分鍵ID_B及び第２の公開鍵y_Bを受信する第１の受信手段１０６と、第１の受信手段１０６により受信した第２の公開鍵y_Bと第１の公開鍵生成手段１０３で用いた素数P_A、原始根g_Aによる巾乗演算を行い、第１の鍵K_Aを生成する第１の秘密鍵生成手段１０７と、第１の鍵K_Aの一部分を部分鍵ID_Aとし、部分鍵ID_Aと部分鍵ID_Bを比較する第１の比較手段１０８と、第１の比較手段１０８による比較の結果、一致する場合には、第１の鍵K_Aのビット列のうち、部分鍵ID_Aにした部分とは異なる一部分を共通鍵K_{AB}として、共通鍵K_{AB}を記憶する第２の記憶手段１０９とを有し、共通鍵生成処理手段２５０は、受信端末２００が、乱数r_Bを生成する第３の乱数生成手段２０１と、送信端末１００から送信された素数P_A，原始根g_A及び公開鍵y_A、及び乱数r_Bにより巾乗演算を行い、第２の公開鍵y_Bを生成する第２の公開鍵生成手段２０３と、第２の公開鍵生成手段２０３で生成された第２の公開鍵y_B、素数P_A、乱数r_Bにより巾乗演算を行い、第２の鍵K_Bを生成する第２の秘密鍵生成手段２０７と、第２の秘密鍵生成手段２０７により生成された第２の鍵K_Bのビット列の一部分を部分鍵ID_Bとし、第２の鍵K_Bのビット列のうち、部分鍵ID_Bに使用した部分以外の一部分を共通鍵K_{AB}として格納する第３の記憶手段２０９と、第２の公開鍵y_B及び部分鍵ID_Bを送信端末１００に送信する第３の送信手段２０９とを有する。

【０００９】また、データ転送処理手段１６０は、送信端末１００が、乱数R_Aを生成する第２の乱数生成手段１１１と、乱数R_Aで第２の記憶手段１０９に格納されているK_{AB}を暗号化し、第１の暗号文Ｅ（K_{AB}，R_A）を生成する第１の暗号化手段１１０と、乱数R_Aで本文Ｍを暗号化し、第２の暗号文Ｅ（Ｍ，R_A）を生成する第２の暗号化手段１１３と、第１及び第２の暗号化手段１１０、１１３で生成された第１の暗号文及び第２の暗号文を送信する第２の送信手段１１４とを有し、データ転送処理手段２６０は、受信端末２００が、送信端末１００から受信した第１の暗号文Ｅ（R_A，K_{AB}）を第３の記憶手段２１０に格納されているK_{AB}を用いて復号し、復号鍵R_Aを取得する第１の復号手段２１３と、復号鍵R_Aを用いて、第２の暗号文Ｅ（Ｍ，R_A）を復号化して本文Ｍを取得する第２の復号手段２１４とを有する。

【００１０】また、上記のデータ転送処理手段１６０、

２６０において、送信端末１００は、本文Mのビット長を所定のビット列に変換し、変換データＭＩＣを送信する変換・送信手段を有し、受信端末２００は、変換データＭＩＣを受信すると、第２の復号化手段２１３により取得した本文Mのビット長を所定のビット列に変換する変換データＭＩＣ’を取得する第１の変換手段と、変換手段により取得したＭＩＣ’と受信した変換データＭＩＣとを比較し、一致するかを判断する第２の比較手段とを更に有する。

【００１１】また、上記のデータ転送処理手段１６０、２６０において、送信端末１００は、本文Mのビット長を所定のビット列に変換し、変換データＭＩＣを生成する第２の変換手段と、変換データＭＩＣと第２の乱数生成手段１１１で生成された乱数R_Aを暗号化し、第３の暗号文Ｅ（ＭＩＣ，R_A）を生成する第３の暗号化手段と、第３の暗号文Ｅ（ＭＩＣ，R_A）を送信する第４の送信手段とを有し、受信端末２００は、第４の送信手段により送信された第３の暗号文Ｅ（ＭＩＣ，R_A）を、第１の復号手段２１３により取得した復号鍵R_Aを用いて第３の暗号文Ｅ（ＭＩＣ，R_A）を復号し、ＭＩＣを取得する第３の復号手段と、第３の復号手段により取得したＭＩＣと、第２の復号手段２１４により取得された本文Mを比較して一致するかを判断する第３の比較手段をさらに有する。

【００１２】図２は、本発明の原理を説明するためのシーケンスチャートである。本発明は、暗号化された文書を送信端末から電子メールで受信端末に送信し、受信端末が送信端末より受信した文書を復号化する暗号通信方法において、最初に、共通鍵生成処理として、送信端末が受信端末に対して、共通鍵を生成するためのデータを送信し（ステップ１）、受信端末が、データを用いて、共通鍵を生成し（ステップ２）、共通鍵の部分鍵を送信端末に送信し（ステップ３）、送信端末は、受信した共通鍵の部分鍵と、送信端末で生成した鍵とを比較して一致していれば、送信端末及び受信端末間において共通に使用する正当な共通鍵として保持し（ステップ４）、次に、データ転送処理として、共通鍵生成手段において、正当な共通鍵であることが確認された後、送信端末は、共通鍵を用いてデータを暗号化して（ステップ５）、受信端末に送信し（ステップ６）、受信端末は、共通鍵を用いて暗号化されたデータを復号する（ステップ７）。

【００１３】また、上記の共通鍵生成処理において、送信端末は、予め、素数P_A、素数P_Aの原始根g_Aを保持しておき、送信端末は、乱数r_Aを生成し、素数P_A、原始根g_Aにより公開鍵y_Bを生成して受信端末に送信し、受信端末は、乱数r_Bを生成し、送信端末より送信された素数Ｐ、原始根ｇにより公開鍵y_Bと鍵K_Bを生成すると共に、共通鍵K_Bのある特定部分のｍビットを共通鍵K_{AB}として保持し、鍵K_Bのｍビット以外のｎビットを部分鍵ID_Bとして、公開鍵y_Bと共に送信端末に送信し、送信端末は、受信端末より受信した公開鍵y_Bと予め保持されている素数P_A、原始根g_Aを用いて鍵K_Aを生成し、鍵K_Aのある特定部分のｎビットを部分鍵ID_Bとし、鍵ID_Aと鍵ID_Bが一致しているかを検査し、一致している場合には、鍵K_Aと鍵K_Bが等しいと見做し、鍵K_Aのある特定部分のｍビットを共通鍵K_{AB}として保持する。

【００１４】また、上記のデータ転送処理において、送信端末は、乱数R_Aを生成し、乱数R_Aで共通鍵K_{AB}を暗号化し、暗号文Ｅ（R_A，K_{AB}）を生成し、乱数R_Aで本文Mを暗号化し、暗号文Ｅ（M，R_A）を生成し、暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（M，R_A）を受信端末に送信し、受信端末は、共通鍵K_{AB}を用いて暗号文Ｅ（R_A，K_{AB}）を復号化して復号鍵R_Aを取得し、復号鍵R_Aにより暗号文Ｅ（M，R_A）を復号し、本文Mを取得する。

【００１５】また、上記のデータ転送処理において、送信端末は、本文Mをある長さのｓビット列に変換し、変換されたデータをデータＭＩＣとし、データＭＩＣを受信端末に送信し、受信端末は、データＭＩＣを受信し、復号化された本文Mをある長さのｓビット列に変換し、変換されたデータＭＩＣ’を取得し、受信したデータＭＩＣとデータＭＩＣ’を比較して一致するか否かを判定する。

【００１６】また、上記のデータ転送処理において、送信端末は、本文Mをある長さのｓビット列に変換し、変換されたデータをＭＩＣとし、乱数R_A及びデータＭＩＣを暗号化し、暗号文Ｅ（ＭＩＣ，R_A）を受信端末に送信し、受信端末は、復号鍵R_Aを取得し、本文Mを取得した後に、本文Mをｓビット列に変換し、変換データＭＩＣ’を取得し、受信した暗号文Ｅ（ＭＩＣ，R_A）を復号した復号文ＭＩＣを取得し、変換データＭＩＣ’と復号文ＭＩＣを比較し、一致するか否かを判定する。

【００１７】

【作用】本発明は、送信端末と受信端末間で共通に有する共通鍵を生成する際に、受信端末で生成した鍵の部分鍵を送信端末に送信し、受信端末はその部分鍵を用いて共通鍵を生成する。これにより、共通鍵を送信端末、受信端末の両端末で共有する際に、通信路をいくつかのデータが通過するが、通信路を監視する第３者は、送信端末が生成する乱数r_Aを知り得ない限り共通鍵K_{AB}を知ることはできない。ここで、素数P_A及び原始根g_Aは通信路を通過するので、第３者がこれらを知ることは可能であるが、この２つの値から乱数r_Aを知ることは不可能である。なぜなら、離散対数問題と呼ばれ、この問題を多項式時間で解く有効なアルゴリズムは知られていないため、安全であるといえる。

【００１８】また、両端末で計算された鍵K_A（＝K_B）の一部分ID_A（＝ID_B）として比較検査するため、送信端末側は鍵の共有が正しく行われたか否かを

確認することができる。この鍵共有は、特に支障のない限り、両端末で一度行うだけでよい。

【００１９】また、データ転送においては、一般に本文Mは、そのデータ長が乱数R_Aより長いことが考えられるため、まず、乱数R_Aでデータを暗号化し、その後、この乱数R_Aを共通鍵K_{AB}で暗号化する。一般に乱数R_Aが本文Mよりデータ長が長いことから、特に複数の受信者へ同一のデータを発信する同報通信時には、処理工程及び処理時間が短縮される。

【００２０】

【実施例】以下、図面と共に、本発明の実施例を詳細に説明する。図３は、本発明の第１の実施例の暗号化装置の構成を示し、図４は、本発明の第１の一実施例の復号化装置の構成を示す。なお、図３、図４において、説明の明瞭化のため、暗号化装置と復号化装置を別個に記載しているが、本来１つの端末装置に両方の機能を具備するものである。

【００２１】図３において、送信側端末である暗号化装置１００（以下、端末Ａ）は、第１の記憶部１０１、第１の乱数生成器１０２、第１の巾乗計算器１０３、第１のデータ送信部１０４、第２の記憶部１０５、データ受信部１０６、第２の巾乗演算器１０７、比較器１０８、第３の記憶部１０９からなる鍵生成部１５０と、第１のデータ暗号化部１１０、第２の乱数生成器１１１、第４の記憶部１１２、第２のデータ暗号化部１１３、及び第２のデータ送信部１１４よりなるデータ転送部１６０から構成される。

【００２２】図４において、復号化装置２００（以下端末Ｂ）は、乱数生成器２０１、第１のデータ受信部２０２、巾乗計算器１０３、第１の記憶部２０４、データ送信部２０５、及び第２の記憶部２０６からなる鍵生成部２５０と、第２のデータ受信部２１２、第１のデータ復号化部２１３、第２のデータ復号化部２１４、及び第３の記憶部２１５よりなるデータ転送部２６０より構成される。

【００２３】なお、上記の図３、図４において、説明の明瞭化のため、同種の構成要素（例えば、送信部）が１つの端末に含まれているが、本来は１つずつの構成でよい。上記の端末Ａの第１の記憶部１０１は、予め、端末毎に定めた素数P_Aとその原始根g_Aを格納しておき、さらに、第３の記憶部１０５は、送信先端末（復号化装置）毎に異なる鍵を共有するため、それらの鍵を格納する。

【００２４】また、送信端末１００と受信端末２００間の通信はメールシステムにより行われるものとする。図５は、本発明の第１の実施例の動作を示すシーケスチャートである。以下、図３、図４に示す各構成要素について図５に沿って説明する。

【００２５】ステップ５０１）　端末Ａの第１の乱数生成器１０２は、５１２ビット長の乱数r_Aを生成して、第１の巾乗計算器１０３に入力する。また、乱数r_Aは、以降の処理で再度使用するため、第２の記憶部１０５に記憶しておく。

ステップ５０２）　第１の巾乗計算器１０３は、第１の記憶部１０１から素数P_Aと原始根g_Aを取り出し、第１の乱数生成器１０２により入力された乱数r_Aを用いて、

【００２６】

【数１】

$$y_A \equiv g_A^{r_A} \bmod P_A$$

【００２７】（但し、上記の式は、P_Aを法とした剰余計算）を計算し、端末Ａの公開鍵y_Aを生成し、素数P_Aと原始根g_Aと共に、第１のデータ送信部１０４に転送する。

ステップ５０３）　第１のデータ送信部１０４は、第１の巾乗計算器１０３より転送された素数P_Aと原始根g_Aと公開鍵y_Aを端末Ｂに送信する。

【００２８】ステップ５０４）　端末Ｂの第１のデータ受信部２０２は、端末Ａから上記のデータを受信すると、第１の乱数生成器２０１により５１２ビットの長さの乱数r_Bを生成する。

ステップ５０５）　端末Ｂは、受信したデータP_Aと原始根g_Aと公開鍵y_Aと乱数r_Bを第１の巾乗計算器２０３に入力し、

【００２９】

【数２】

$$y_B \equiv g_A^{r_B} \bmod P_A$$

【００３０】（但し、上記の式は、P_Aを法とした剰余計算）を計算し、端末Ｂの公開鍵y_Bを取得する。さらに、

【００３１】

【数３】

$$K_B \equiv y_A^{r_B} \bmod P_A \equiv g_A^{r_A r_B} \bmod P_A$$

【００３２】（但し、上記の式は、P_Aを法とした剰余計算）を計算し、鍵K_Bを求める。

ステップ５０６）　次に、鍵を正しく共有化しているかを参照するための識別子として、鍵K_Bを２進数表示した際の０桁目から６３桁目までをID_Bとし、また、端末Ａと端末Ｂとの共通鍵として、６４桁目から１２７桁目までをK_{AB}として設定し、第２の記憶部２０６に記憶する。

【００３３】ステップ５０７）　端末Ｂは、第１の記憶部２０４から宛先である端末Ａのアドレスを参照し、端末Ａに対して、鍵y_Bと識別子ID_Bをデータ送信部２０９を介して端末Ａに送信する。

ステップ５０８）　端末Ａのデータ受信部１０６は、端末Ｂから鍵y_Bと識別ID_Bを受信すると、第２の記憶部１０５に格納されている乱数r_Aを取り出し、第２の

巾乗計算器１０７に入力して、

【００３４】

【数４】

$$K_A \equiv y_B^{\wedge} \mod P_A \equiv g_A^{r_A \cdot r_B} \mod P_A$$

【００３５】（但し、上記の式は、P_Aを法とした剰余計算）により鍵K_Aを求める。

ステップ５０９）　上記の巾乗演算により求められた鍵K_Aにより、鍵を正しく共有化しているかの識別子として、図６に示すように、K_Aを２進数表記した場合の０桁目から６３桁目（６４ビット）を識別子ID_Aとし、端末Ｂより受信した識別子ID_Bと識別子ID_Aを比較器１０８に入力して比較する。等しい場合は、端末Ａと端末Ｂとで、$K_A = K_B$であることが確認できる。図６の例では、５１２ビットのビット列を有するデータのうち、６４ビットのＩＤ識別用６０１を用いて端末Ａと端末ＢとのＩＤを比較し、同一であれば、次の６４ビットの共通鍵６０２をK_{AB}として記憶しておくものである。

【００３６】ステップ５１０）　上記のステップ５０９で$K_A = K_B$が確認できた場合には、６４桁目から１２７桁目までを共通鍵K_{AB}として、第３の記憶部１０９に格納する。なお、上記の処理は、どちらかの端末から明示的に鍵を変更することをしない限り、ステップ５０１～ステップ５１０の処理は、最初に１度だけ実行しておき、記憶部に格納しておけばよい。

【００３７】次に、端末Ａと端末Ｂ間のデータ転送について説明する。

ステップ５１１）　端末Ａの第２の乱数生成器１１１は、乱数R_Aを生成し、第１のデータ暗号化部１１０及び第２のデータ暗号化部１１３に入力する。

ステップ５１２）　第２の記憶部２０６から共通鍵K_{AB}を読み出して、第１のデータ暗号化部１１０に入力し、乱数R_Aを用いて共通鍵K_{AB}を暗号化し、暗号文Ｅ（R_A, K_{AB}）を取得する。

【００３８】ステップ５１３）　第２のデータ暗号化部１１３は、本文Ｍが入力され、乱数R_Aにより暗号化し、暗号文Ｅ（Ｍ，R_A）を取得する。

ステップ５１４）　第１のデータ暗号化部１１０は、暗号文Ｅ（R_A，K_{AB}）を、第２のデータ暗号化部１１３は、暗号文Ｅ（Ｍ，R_A）を第２のデータ送信部１１４に転送し、第２のデータ送信部１１４は、暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（Ｍ，R_A）を端末Ｂに転送する。

【００３９】ステップ５１５）　端末Ｂの第２の受信部２１２は、端末Ａから送信された暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（Ｍ，R_A）を受信し、暗号文Ｅ（R_A，K_{AB}）を第１の復号化部２１３に入力し、第２の記憶部２１０より共通鍵K_{AB}を取り出して第１の復号化部２１３に入力して、復号化し、復号鍵としてR_Aを取得する。

【００４０】ステップ５１６）　次に、復号鍵R_Aを第２の復号化部２１４に入力し、暗号文Ｅ（Ｍ，R_A）を復号し、元の本文Ｍを取得する。

次に、データ転送処理の他の例を以下に示す。図８は、本発明の第２の実施例のデータ転送部の構成を示す。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。端末Ａにおいて、本文Ｍをｓビット列に変換するためのデータ変換部１１６を第１の実施例の図３のデータ転送部１６０の構成に加えた構成である。また、端末Ｂにおいても同様に本文Ｍをｓビット列に変換するためのデータ変換部２１６と、端末Ａから受信したデータとデータ変換部２１６で変換されたデータを比較するための比較部２１７をデータ転送部２６０に加えた構成である。

【００４１】図９は、本発明の第２の実施例のデータ転送動作を示すシーケンスチャートである。上記の第１の実施例の図７に示すシーケンスチャートと同様の動作については、同一のステップ番号を付す。

ステップ５１１）　端末Ａの第２の乱数生成器１１１は、乱数R_Aを生成し、第１のデータ暗号化部１１０及び第２のデータ暗号化部１１３に入力する。

【００４２】ステップ５１２）　第２の記憶部２０６から共通鍵K_{AB}を読み出して、第１のデータ暗号化部１１０に入力し、乱数R_Aを用いて共通鍵K_{AB}を暗号化し暗号文Ｅ（R_A, K_{AB}）を取得する。

ステップ５１３）　第２のデータ暗号化部１１３は、本文Ｍが入力され、乱数R_Aにより暗号化し、暗号文Ｅ（Ｍ，R_A）を取得する。

【００４３】ステップ５１３－１）　次に、データ変換部１１６は、本文Ｍをｓビット列に変換し、変換されたデータをＭＩＣとする。変換されるビット列は任意に設定可能である。

ステップ５１４－１）　第１のデータ暗号化部１１０は、暗号文Ｅ（R_A，K_{AB}）を、第２のデータ暗号化部１１３は、暗号文Ｅ（Ｍ，R_A）を第２のデータ送信部１０４に転送し、第２のデータ送信部１１４は、暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（Ｍ，R_A）を端末Ｂに転送する。さらに、データ変換部１１６で変換されたデータＭＩＣも合わせて送信する。

【００４４】ステップ５１５）　端末Ｂの第２の受信部２１２は、端末Ａから送信された暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（Ｍ，R_A）及びデータＭＩＣを受信し、暗号文Ｅ（R_A，K_{AB}）を第１の復号化部２１３に入力し、第２の記憶部２１０より共通鍵K_{AB}を取り出して第１の復号化部２１３に入力して、復号化し、復号鍵としてR_Aを取得する。

【００４５】ステップ５１６）　次に、復号鍵R_Aを第２の復号化部２１４に入力し、暗号文Ｅ（Ｍ，R_A）を復号し、元の本文Ｍを取得する。

ステップ５１６－１）　データ変換部２１６は、ステップ５１６で復号された本文Ｍを任意のビット列ｓビット

に変換し、データＭＩＣ’とする。

【００４６】ステップ５１６－２）　データ変換部２１６の出力であるＭＩＣ’と、第２のデータ受信部２１２で受信したＭＩＣを比較部２１７に入力し、ＭＩＣ’とＭＩＣを比較し、一致しているか否かを判定する。このような方法によっても受信したデータが正しいか否かの判断が可能である。

【００４７】図１０は、本発明の第３の実施例のデータ転送部の構成図である。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。端末Ａにおいて、本文Ｍをｓビット列に変換するためのデータ変換部１１６と、第２の乱数生成器１１１で生成された乱数R_Aを用いて、データ変換部１１６で変換されたデータを暗号化する第３のデータ暗号化部１１７を第１の実施例の図３のデータ転送部１６０に加えた構成である。また、端末Ｂにおいては、第２のデータ受信部２１２で受信した暗号化文のうち、上記の第２のデータ暗号化部１１７の出力である暗号文を復号する第３のデータ復号部２１８と、第２のデータ復号化部２１４で復号されたデータの任意のｓビットの長さのデータに変換するデータ変換器２２０と、データ変換器２２０で変換されたデータと第３のデータ復号部２１８で復号されたデータを比較するための比較部２１９が図４のデータ転送部２６０に加えた構成である。

【００４８】図１１は、本発明の第３の実施例のデータ転送動作を示すシーケンスチャートである。同図において、上記の第１の実施例の図７と同様の動作については、同一のステップ番号を付す。

ステップ５１１）　端末Ａの第２の乱数生成器１１１は、乱数R_Aを生成し、第１のデータ暗号化部１１０及び第２のデータ暗号化部１１３に入力する。

【００４９】ステップ５１２）　第２の記憶部２０６から共通鍵K_{AB}を読み出して、第１のデータ暗号化部１１０に入力し、乱数R_Aを用いて暗号文Ｅ（R_A, K_{AB}）を取得する。

ステップ５１３）　第２のデータ暗号化部１１３は、本文Ｍが入力され、乱数R_Aにより暗号化し、暗号文Ｅ（Ｍ，R_A）を取得する。

【００５０】ステップ５１３－１０）　データ変換部１１６は、本文Ｍをｓビット列に変換し、変換されたデータをＭＩＣとする。

ステップ５１３－１１）　第３のデータ暗号化部１１７は、変換されたデータＭＩＣを乱数R_Aを用いて暗号化し、暗号文Ｅ（ＭＩＣ，R_A）を取得する。

【００５１】ステップ５１４－１０）　第２のデータ送信部１１４は、暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（Ｍ，R_A）及び暗号文Ｅ（ＭＩＣ，R_A）を端末Ｂに転送する。

【００５２】ステップ５１５）　端末Ｂの第２の受信部２１２は、端末Ａから送信された暗号文Ｅ（R_A，K_{AB}）と暗号文Ｅ（Ｍ，R_A）及び暗号文Ｅ（ＭＩＣ，R_A）を受信し、暗号文Ｅ（R_A，K_{AB}）を第１の復号化部２１３に入力し、第２の記憶部２１０より共通鍵K_{AB}を取り出して第１の復号化部２１３に入力して、復号化し、復号鍵R_Aを取得する。

【００５３】ステップ５１６）　復号鍵R_Aで暗号文Ｅ（Ｍ，R_A）を復号し、本文Ｍを取得する。

ステップ５１６－１０）　復号された本文Ｍをデータ変換器２２０に入力し、ｓビット列のデータに変換し、変換データＭＩＣ’を得る。

【００５４】ステップ５１６－２０）　第３のデータ復号化部２１８は、復号鍵R_Aで暗号文Ｅ（ＭＩＣ，R_A）を復号し、データＭＩＣを取得する。

ステップ５１６－３０）　変換データＭＩＣ’と復号されたデータＭＩＣを比較部２１９に入力し、比較し、同一であるか否かを判断する。

【００５５】上記の第３の実施例も第２の実施例と同様に、受信側で受信したデータの正当性をチェックすることが可能となる。なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００５６】

【発明の効果】上述のように本発明によれば、送信端末、受信端末共に鍵を共有し、データを暗号化して送受信するものであり、鍵の共有化を行う段階では、通信路上に共通鍵K_{AB}が流れないこと、さらに、データ本文が暗号化されて通信路上を流れるために、通信路上を監視する第３者への情報の漏洩が発生しない。

【００５７】また、鍵を共有する段階において、受信端末から共通鍵の一部を送信端末に送信し、送信端末において、比較検査することより、鍵の共有が正しくなされたか否かの検査が可能となるため、鍵の共有化がなされていないままデータを送信する無駄な操作が減少する。

【００５８】また、データ本文を直接共通鍵で暗号化せず、乱数を用いて暗号化したのち、乱数を共通鍵で暗号化することは、データ本文の長さが長い場合、その暗号化に時間がかかるために、特に、同報通信を行う際に処理時間が短縮され、効率的である。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の原理を説明するためのシーケンスチャートである。

【図３】本発明の第１の実施例の暗号化装置（端末Ａ）の構成図である。

【図４】本発明の第１の実施例の復号化装置（端末Ｂ）の構成図である。

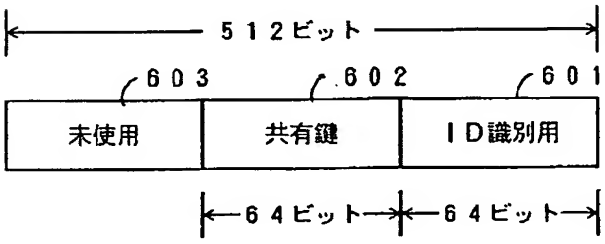
【図５】本発明の第１の実施例の鍵生成動作を示すシーケンスチャートである。

【図６】共通鍵検証に用いるビット列の例を示す図である。

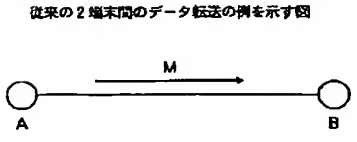
【図７】本発明の第１の実施例のデータ転送動作を示すシーケンスチャートである。
【図８】本発明の第２の実施例のデータ転送部の構成図である。
【図９】本発明の第２の実施例のデータ転送動作を示すシーケンスチャートである。
【図１０】本発明の第３の実施例のデータ転送部の構成図である。
【図１１】本発明の第３の実施例のデータ転送動作を示すシーケンスチャートである。
【図１２】従来の２端末間のデータ転送の例を示す図である。
【図１３】従来の端末群内におけるデータの例を示す図である。
【符号の説明】
１００　送信端末
１０１　第１の記憶手段、第１の記憶部
１０２　第１の乱数生成手段、第１の乱数生成器
１０３　第１の公開鍵生成手段、第１の巾乗計算器
１０４　第１の送信手段、第１のデータ送信部
１０５　第２の記憶部
１０６　第１の受信手段、データ受信部
１０７　第１の秘密鍵生成手段、第２の巾乗計算器
１０８　比較手段、比較器
１０９　第２の記憶手段、第３の記憶部
１１０　第１の暗号化手段、第１のデータ暗号化部
１１１　第２の乱数生成手段、第２の乱数生成器
１１３　第２の暗号化手段、第２のデータ暗号化部
１１４　第２の送信手段、第２のデータ送信部
１１６　データ変換部
１１７　第３のデータ暗号化部
１５０　鍵生成手段、鍵生成部
１６０　データ転送手段、データ転送部
２００　受信端末
２０１　第３の乱数生成手段、乱数生成器
２０２　第１のデータ受信部
２０３　第２の公開鍵生成手段、巾乗演算器
２０４　第１の記憶部
２０５　データ送信部
２０６　第２の記憶部
２０７　第２の秘密鍵生成手段
２０８　第３の記憶手段
２０９　第３の送信手段
２１２　第２のデータ受信部
２１３　第１の復号手段、第１のデータ復号化部
２１４　第２の復号手段、第２のデータ復号化部
２１５　第３の記憶部
２１６　データ変換部
２１７　比較部
２１８　第３のデータ復号化部
２１９　比較部
２２０　データ変換器
２５０　鍵生成手段、鍵生成部
２６０　データ転送手段、データ転送部
６０１　ＩＤ識別用ビット
６０２　共通鍵用ビット
６０３　未使用ビット

【図６】

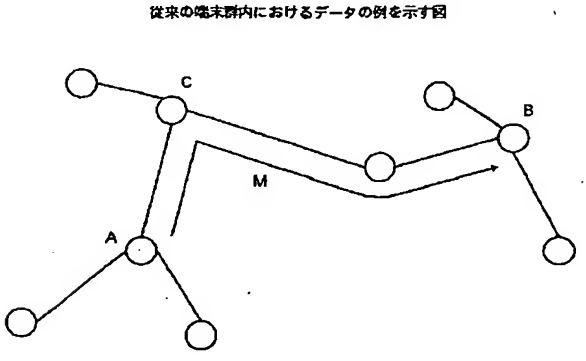
共有鍵検証に用いるビット列の例



【図１２】

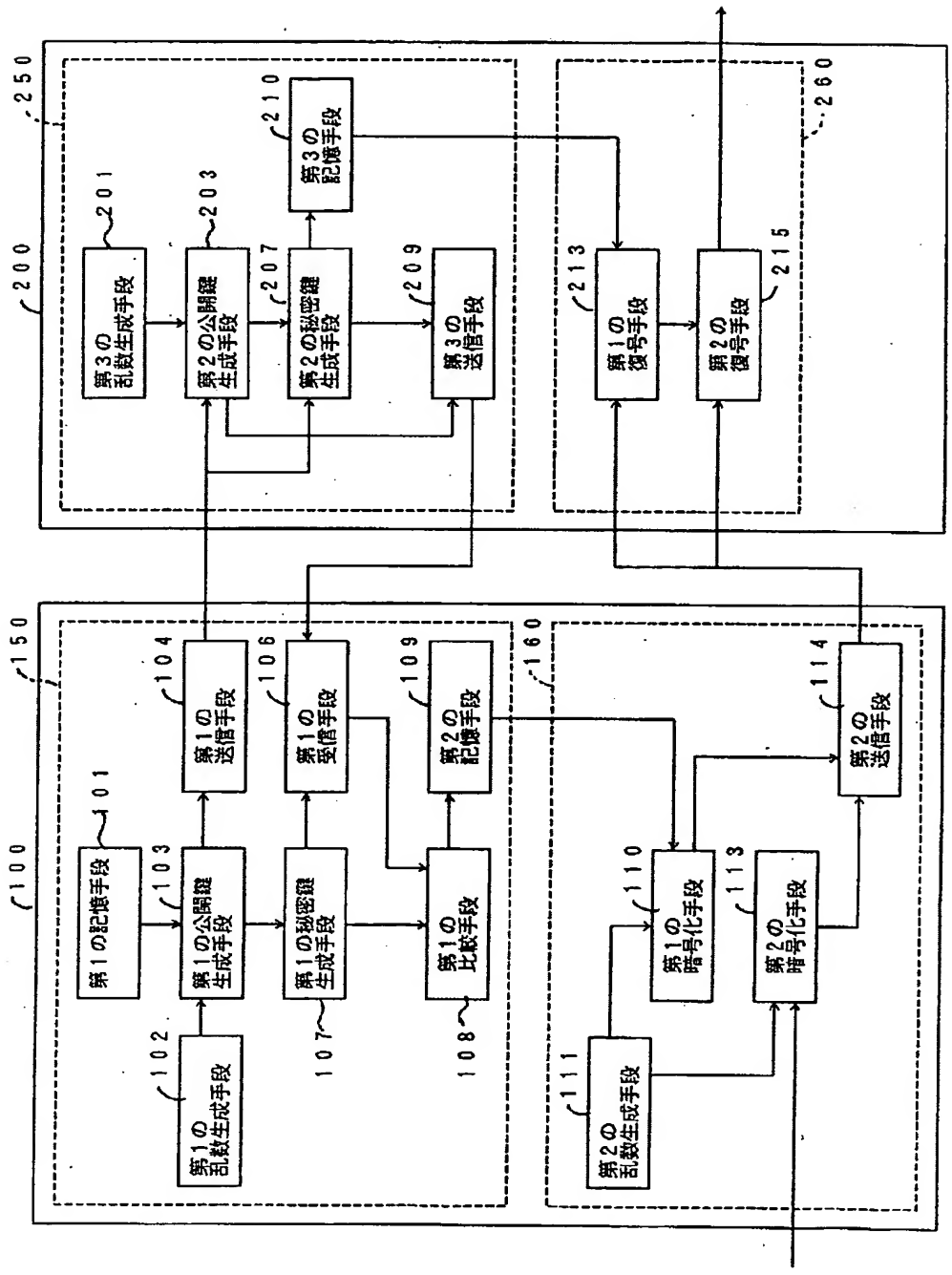


【図１３】



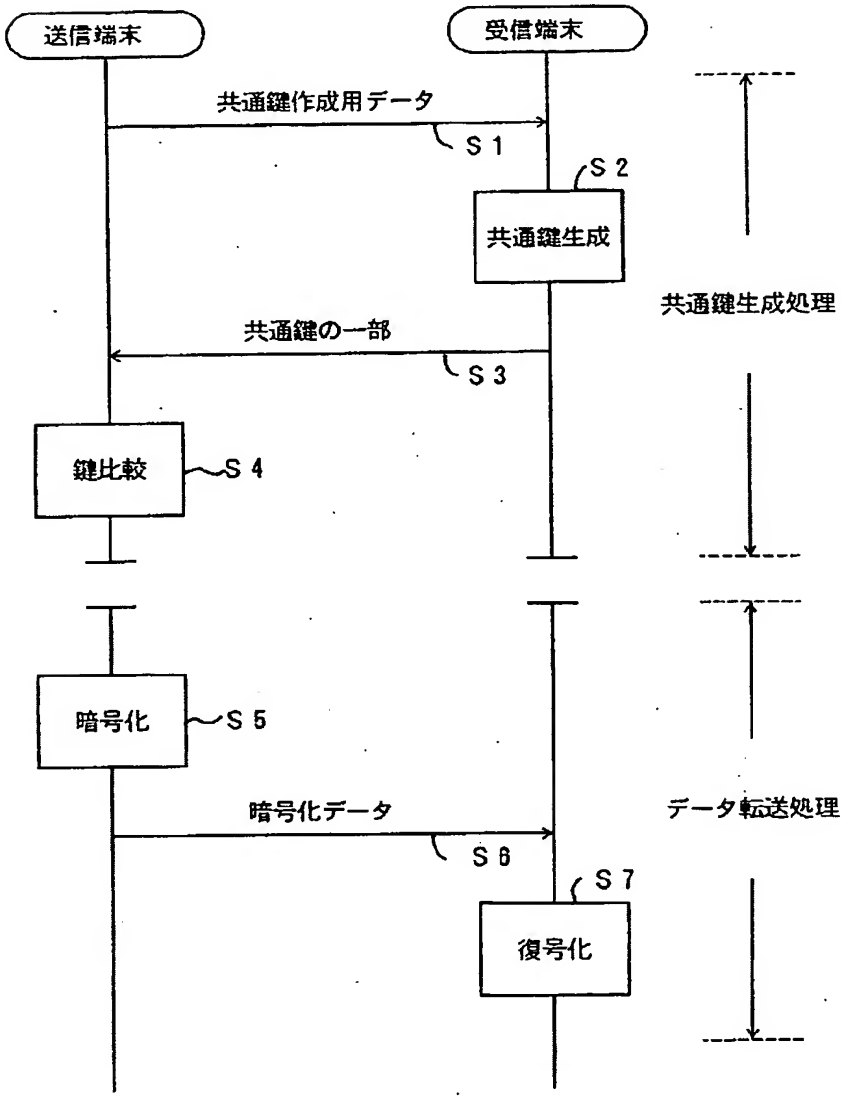
【図１】

本発明の原理構成図



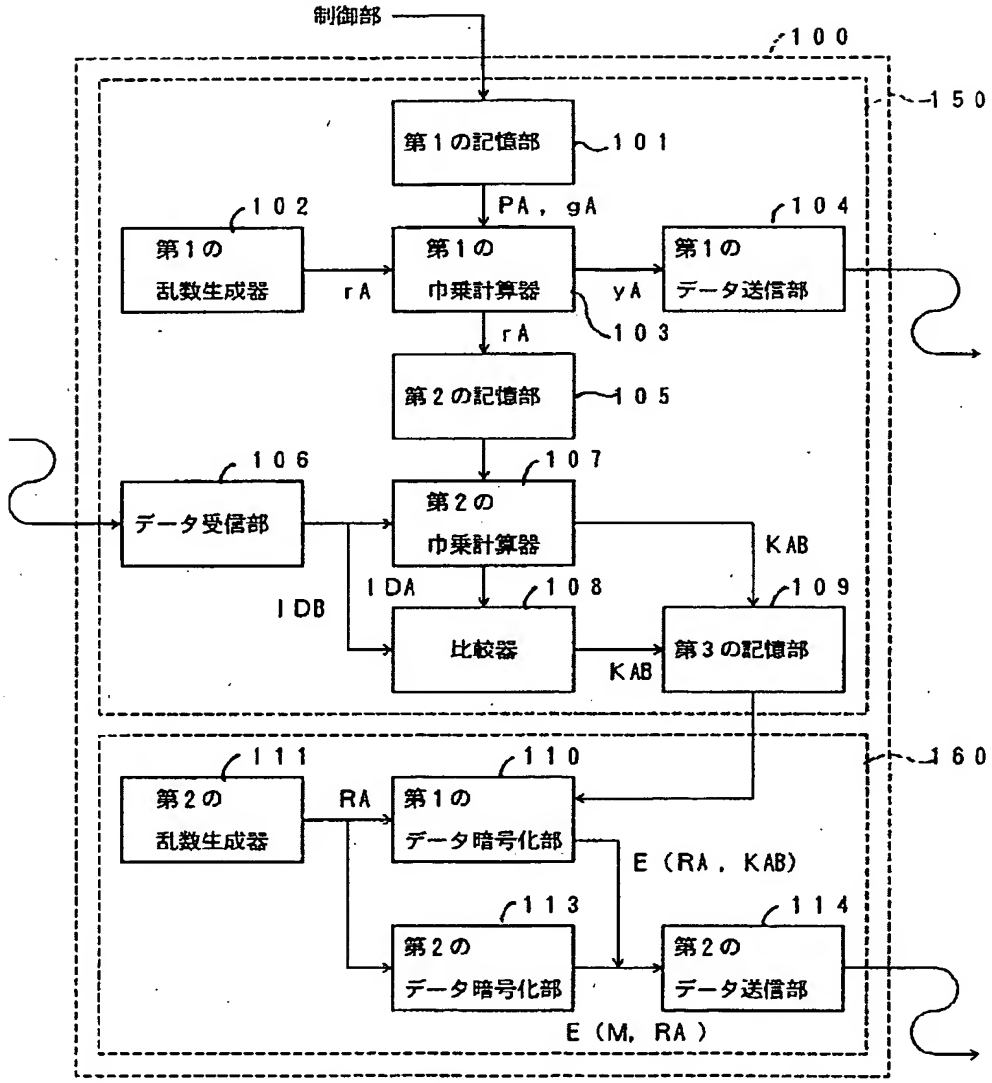
【図２】

本発明の原理を説明するためのシーケンスチャート



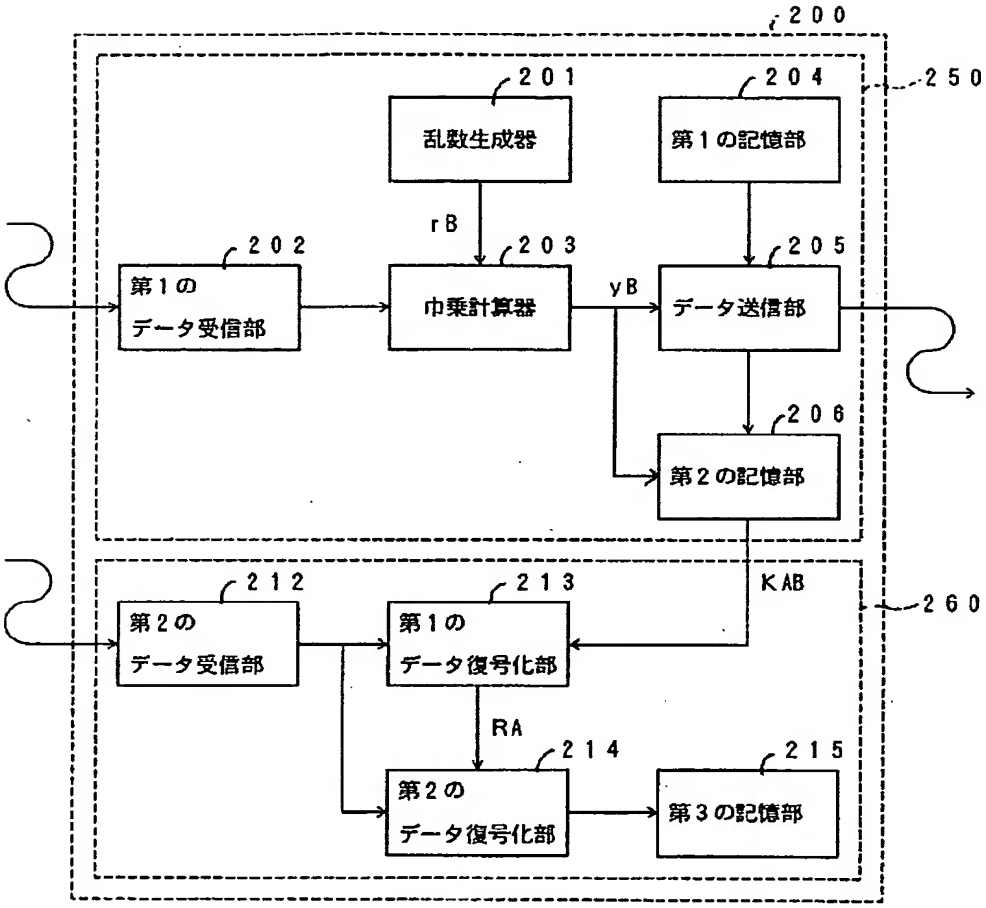
【図３】

本発明の第１の実施例の暗号化装置（端末Ａ）の構成図



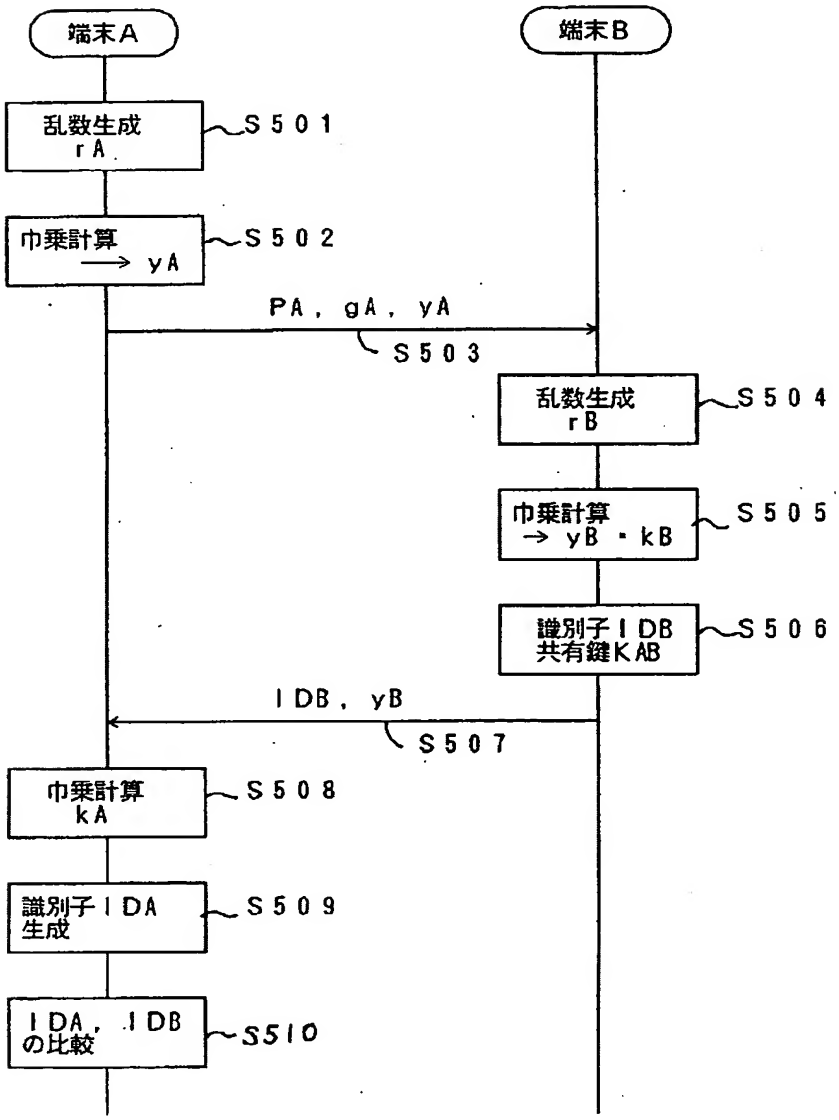
【図４】

本発明の第１の実施例の復号化装置（端末Ｂ）の構成図



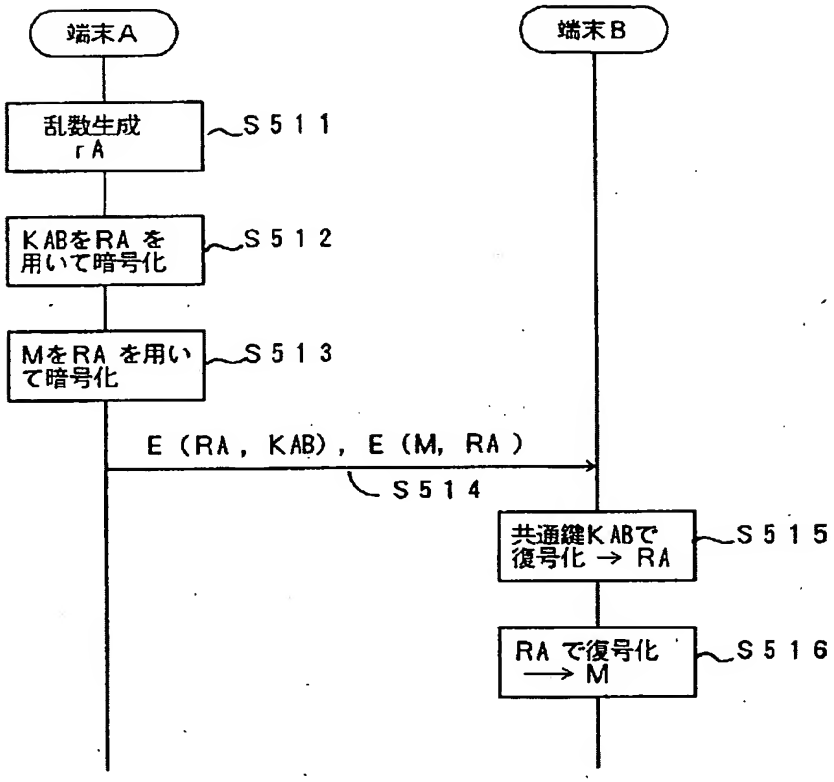
【図５】

本発明の第１の実施例の鍵生成動作を示すシーケンスチャート



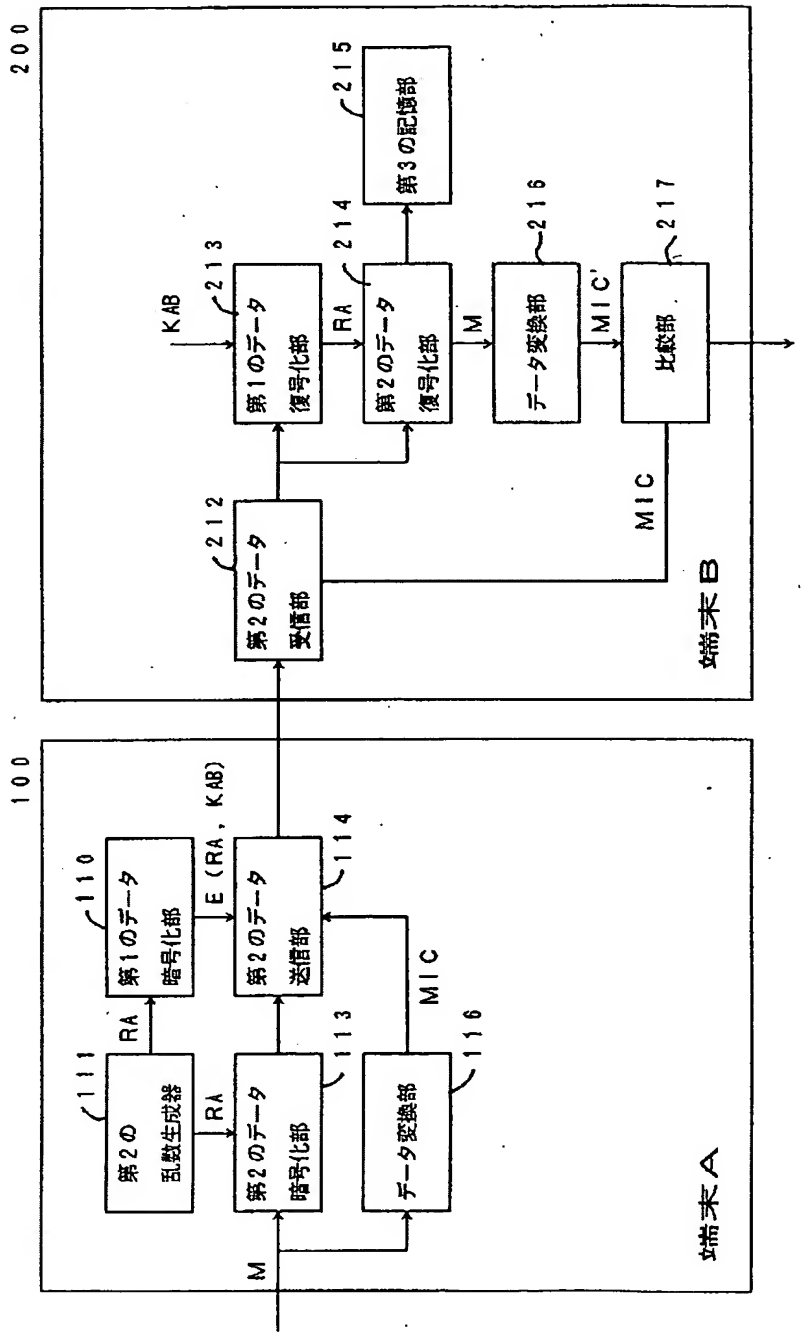
【図７】

本発明の第１の実施例のデータ転送動作を示すシーケンスチャート



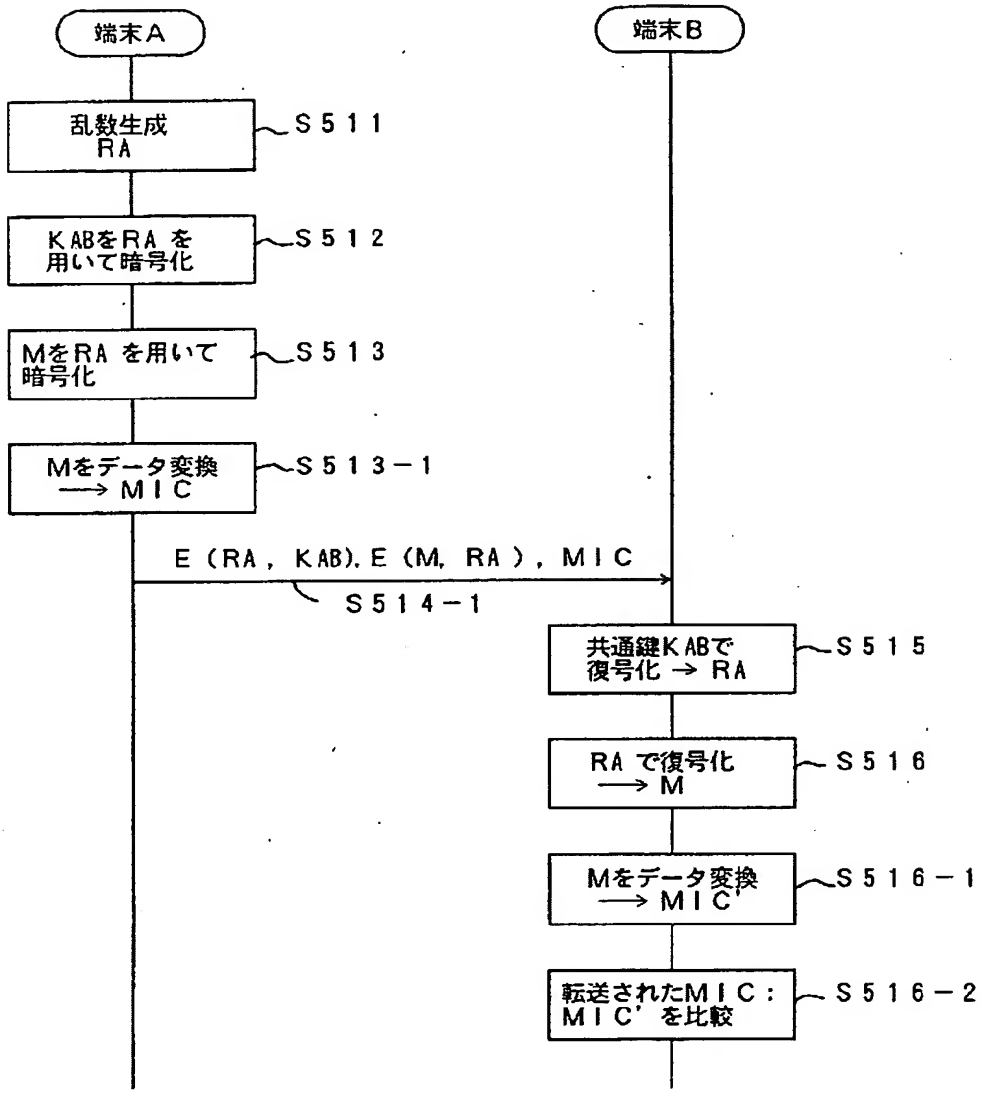
【図８】

本発明の第２の実施例のデータ転送部の構成図



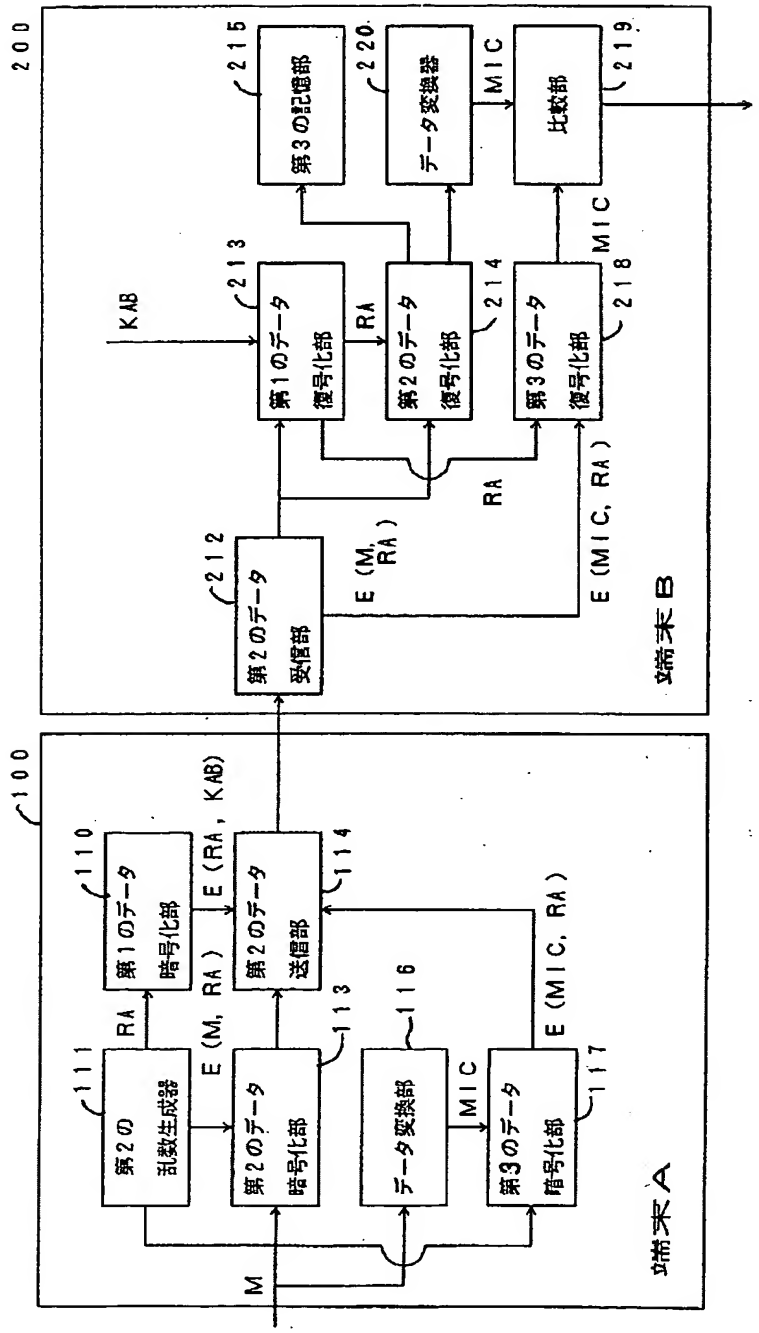
【図９】

本発明の第２の実施例のデータ転送動作を示すシーケンスチャート



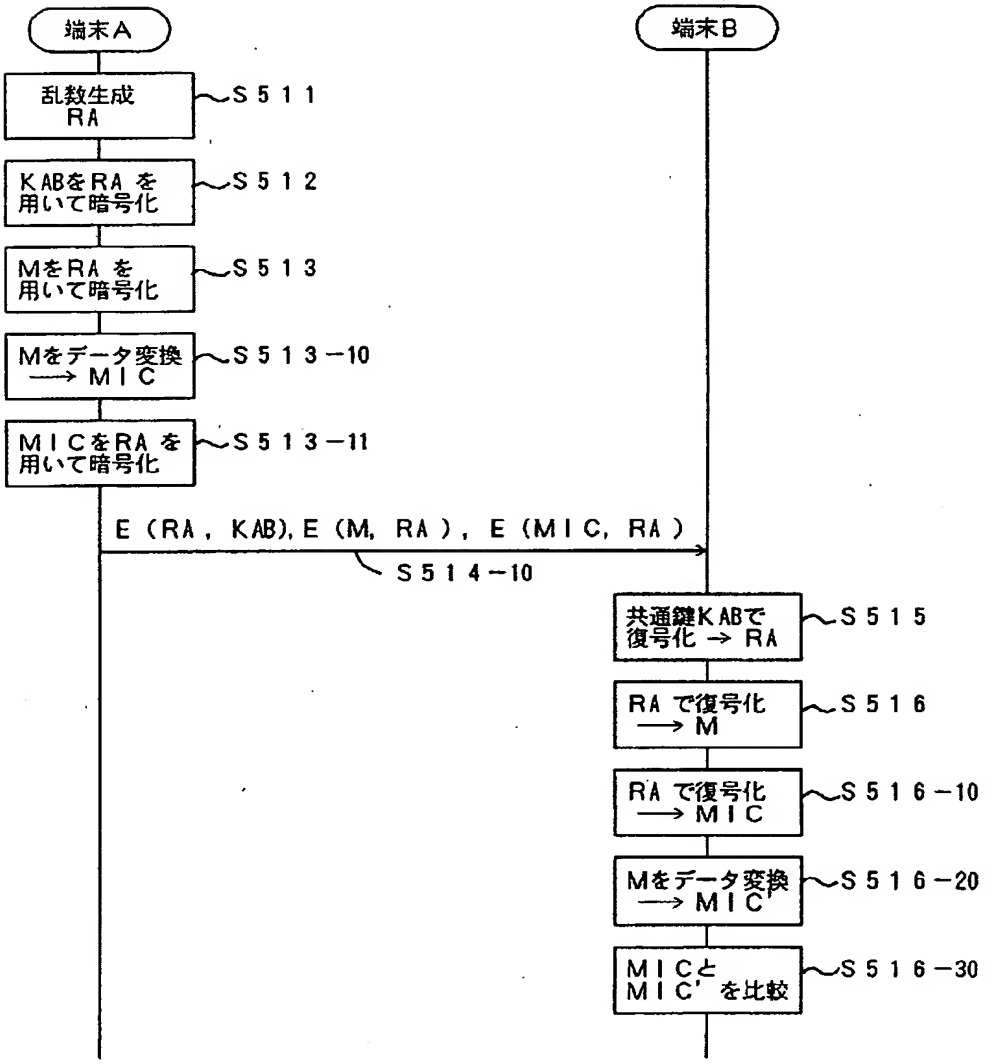
【図１０】

本発明の第３の実施例のデータ転送部の構成図



【図１１】

本発明の第３の実施例のデータ転送動作を示すシーケンスチャート



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　12/54				
12/58				
12/22				
// Ｇ０９Ｃ　1/00		7259－5Ｊ		
		9466－5Ｋ	Ｈ０４Ｌ　11/26	

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.